



Policy 9.5	Identity Protection		
<u>Effective Date:</u> 5/24/11	<u>Applicable Law/Statute:</u> CB-0030-11	<u>Source Doc/Dept.:</u> None/HR	<u>Authorizing I.C. Sec.:</u> None
<u>Last Amended Date:</u> 2/28/12			

IDENTITY PROTECTION

9.5

POLICY

It is the policy of DuPage County to maintain practices in compliance with applicable laws and regulations in order to protect the identity of employees, persons doing business with the County and persons receiving services from or through the County.

ELIGIBILITY

- All employees of DuPage County shall adhere to the guidelines of this policy. This policy may be applied by the Elected Officials to their employees.

GUIDELINES

A. Protection of social security numbers under the Illinois Identity Protection Act

1. Restricted Access and Use

a. In General

1. Where feasible, the County will use only the last four digits of a Social Security number.
2. The County will not require an individual to submit a Social Security number over the internet unless encryption is available.
3. Paper documents containing Social Security numbers will be stored in locked files or restricted areas. Social Security numbers retained in electronic format or entered into on-line databases will be protected through limited password access, encryption or other appropriate means for securing the data.
4. The County will not print an individual's Social Security number on any ID card or other card required for the individual to access products or services provided by the County
5. The County will not, unless otherwise provided by statute, print an individual's Social Security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery. If otherwise permitted, any such mailing or delivery will be enclosed in an envelope.

b. By County Employees

1. Only employees who are required by their job duties to use or handle Social Security numbers are permitted to have access to such Social Security numbers. Employees will take care not to post or display a Social Security number except as necessary in the performance of their duties. The Care Center will only obtain Social Security numbers as allowable under the Healthcare Portability and Accountability Act (HIPPA).

c. By the Public

- 1 Social Security numbers, including partial Social Security numbers, will not be publicly posted or publicly displayed in any manner.
- 2 Social Security numbers, including partial Social Security numbers, contained in a public record, including records in electronic format, will be collected and recorded in a manner to permit the Social Security number to be easily redacted for purposes of a Freedom of Information Act request or other proper dissemination of a record.

1. Permitted collection, use and disclosure of Social Security numbers

a. Collection, use or disclosure of Social Security numbers is permitted in the following circumstances:

1. Where necessary in order for the County to perform its duties and responsibilities.
2. Pursuant to a court order, warrant, or subpoena.
3. Where necessary to ensure the safety of State and local government employees and others as provided by statute.
4. For internal verification or administrative purposes.
5. To any entity for the collection of delinquent child support or of any State debt.
6. To a governmental agency to assist with an investigation or the prevention of fraud.

b. Collection or use of Social Security numbers is permitted where necessary or useful to locate a missing person, a lost relative, or a person who is due a benefit, or where otherwise statutorily permitted.

2. Statement of purpose

- a. Upon request by the individual, a statement of the purpose or purposes for which the County is collecting and using the individual's Social Security number will be provided.**

3. Exclusions

- a. This section of the Policy does not apply to the collection, use, or disclosure of a Social Security number as required by State or federal law, rule, or regulation.
- b. This section of the Policy does not apply to documents that are recorded with the County Recorder.

B. Identity Theft Protection under the Fair and Accurate Credit Transaction Act (FACT)

1. General

- a. This section of the Policy is for the protection of covered accounts, defined as those which permit multiple payments or transactions, including but not limited to utility accounts. It applies to business, personal and household accounts established with or by the County.
- b. As used in the Policy, “private identifiers” means any data which would allow the identification of an individual. The term includes but is not limited to credit card numbers, information such as number, expiration date, cardholder name and address, and card security code; service account information such as name, address phone, e-address, date of birth, and account number.
- c. To the greatest extent possible, the County will afford private identifiers the same protections as Social Security numbers.

2. Description of Red Flags

- a. Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft. The County identifies the following red flags in regard to covered accounts:
 - 1. Suspicious documents, such as
 - an application or supporting documents appearing to be altered, forged or destroyed and reassembled
 - those where the photograph or physical description does not match the applicant or card holder
 - those containing other information which is inconsistent with that provided by the applicant or account holder or with other information the County has on file
 - 2. Suspicious personal identifying information, such as
 - information associated with known fraudulent activity
 - information of a type commonly associated with fraudulent activity (e.g., use of a mail drop, prison address, fictitious address, etc.: invalid phone number or pager/answering service)
 - information that is the same as information submitted by another
 - information limited to that which could be readily obtained through public sources or from a stolen wallet

3. Unusual or suspicious activity associated with a covered account, such as
 - use of the account consistent with patterns of fraud (e.g., failure to make first payment, initial payment only)
 - change in pattern of account use (e.g., nonpayment on an account which has no prior history of nonpayment; change in service use)
 - mail returned where account transaction continue
 - notice of non-receipt of paper statement or unauthorized account activity

- b. The County will detect Red Flags by employee review of documents and personal identifying information supplied at the time of the initial application or any account changes. The County will, in the purchase and development of financial software, specify functions to alert for unusual or suspicious documents, identifying information or activity

- c. The County will respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft. A determination will be made by the relevant supervisor or Department Head whether the attempted transaction or activity is likely fraudulent or authentic. If fraudulent, action may include
 1. continued monitoring for evidence of identity theft
 2. contacting the customer
 3. refusal to open a new account or close an existing account
 4. re-opening an existing account with a new number
 5. referral to law enforcement
 6. discontinuance of collection

- C. Implementation of the Identity Theft Protection Program will be directed by the County Administrator who will receive annual reports from those departments having transactions in covered accounts and will be responsible for provisions of training of staff who deal with covered accounts.

PROCEDURES

1. Only employees who are required to use documents containing Social Security numbers will have access to such information.
2. Proper facilities and equipment will be provided to safeguard documents containing Social Security numbers and other private identifiers.
3. All employees who have access to Social Security numbers and other private identifiers – whether received in verbal, written or electronic form – as part of their job duties will be trained to protect the confidentiality of the Social Security number. Training will include instruction on the proper handling of information that contains Social Security

numbers and other private identifiers from the time of collection through the destruction of the information. Training will also include, where appropriate, instruction in recognizing and responding to red flags.

4. This policy will be reviewed and updated as necessary to conform with technology which may affect the security of Social Security numbers and other private identifiers
5. Misuse of any identity-related data will subject the employee to appropriate disciplinary action, not to exclude termination.